30/01/2018

Comment on White Paper on Data Protection Framework for India

Study Group on Data Protection Framework in India (Mandira Narain, Nishtha Sinha, Ianosha Majaw, P. Puneeth and Nupur Chowdhury).

Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Mehrauli Road, New Delhi: 110067.

Corresponding email address: nupur@jnu.ac.in

Disclaimer: Views expressed are the personal views of the members of the Study Group and does not reflect that the Centre for the Study of Law and Governance, JNU.

I. Introduction

The foundational principle for the data protection framework in India is the right to privacy which has been recognized as a fundamental right under the Constitution of India in the *Justice K S Puttaswamy v. Union of India* [(2017) 10 SCC 1]. This therefore constitutes the fundamental legal basis for the enactment of the data protection framework in India. Further the legal basis for this legislation can also be drawn from India's international commitments under the Universal Declaration of Human Rights (Article 12 of UDHR recognizes the right to privacy)[1] andInternational Covenant on Civil and Political Rights (Article 17 of the ICCPR recognizes the right to privacy).[2] It is important to stress that India is a signatory to these international legal instruments and has not made any reservations to these specific clauses and is therefore legally committed to enact a domestic legislation. Article 253 powers Parliament to enact legislations to implement its international treaty obligations. By virtue of the said provision, Parliament has competence to enact a domestic data protection law. It is important to explicitly state these international legal instruments as well as the *Puttaswamy* judgement as the philosophical basis for enacting the data protection law. This will also aid in the interpretation of the parent statute.

Apart from the four propositions of law explicitly and unanimously laid down in conclusion *vide* 'order of the court', in *Justice K S Puttaswamy v. Union of India,* it is important to cull out and consider majority views in the judgment. The views expressed by the majority, though in separate judgments, are as much good law as that of the 'order of the court' in that reflects the unanimous view of the bench.The views of the majority that can be culled out from different judgments throw enough light on the nature, scope, contours and implications of the fundamental right to privacy. The following points have been culled out from different judgmentsrendered in the case as majority view:

- Human dignity is the foundational aim of the protection of the right to privacy. The right to privacy essentially protects the spatial, informational and decisional autonomy of the individual. The right to self expression is at the core of the protection of the right to privacy.
- There are positive and negative aspects to the constitutional protection of the right to privacy. State is under a negative obligation not to take away or undermine the right to privacy except in accordance with the provisions of

[1] Article 12 states that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' Universal Declaration of Human Rights.

[2] Article 17 (1) provides that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honourand reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.'

law as envisaged under Article 21 of the Constitution of India. The state is also under a positive obligation to protect the right to privacy *inter se* amongst private persons. The right to privacy is a specific kind of fundamental right that by clear implication provides for the horizontal application of this fundamental right.

- The safeguards doctrine as was laid down in the*District Registrar and Collector, Hyderabad v.Canara Bank*[3] is an essential aspect of the right to privacy. This entails the recognition of three important principles. First, the principle of 'reasonable expectation of privacy' as the guiding rule in determining when privacy was expected and found violated. Second, that even in cases when private information is shared that information, the entity collecting such information is under a legal obligation to safeguard that information from third party disclosure and integrity of the information. Third, excessive delegation of the statutory power to collect information (allowing for instance delegation of the power to non-governmental persons) may compromise privacy and therefore would violate the right to privacy and is therefore prohibited.
- International commitments can be a source of fundamental rights in the Constitution of India specifically when there is no conflicting constitutional or domestic statutory bar and the Court is then allowed greater space to apply the principle of harmonious construction.
- Privacy of mind and body and specifically family, marriage, procreation and sexual orientation have been explicitly determined to be aspects of one's life that is protected from invasion by state and other non-state actors on grounds of violation of privacy.

All these points have to be given due consideration and thought and should guide both the design and the substantive content of the data protection law.

II. General Principles of the Data Protection Framework

1. Data Authorship – the law should clearly state the principle that the right to privacy is a fundamental right of the individual and therefore complete authorship/ownership and control of the usage of any personal data shall vest with the individual.

2. Informed Consent – Consent is an expression of human dignity and autonomy of choice. For such expression to be genuine, it has to be informed, explicit and meaningful. Following from that, a person should have the right not to give consent and no undue disadvantage should result from the denial of consent. Both in cases where consent is given voluntarily and in case of non-consensual collection of data for extraordinary purposes like national security, no harm, undue disadvantage, prejudice, less favourable treatment should result from that collection or processing of the data.

3. Holistic Application – the law must apply to both private sector entities and government. Specific exemptions may be carved out for non-consensual collection of data by government in specific instances in the public interest.

[3] AIR 2005 SC 186

4. Transparency and fairness – data collection, data processing, and data disclosure should be lawful, fair and transparent. The principle of transparency would require that all collection, processing and disclosure of data should be undertaken in a manner wherein information is communicated in a clear, simple and in an understandable language. Individuals have the right to know when data about them is collected, processed or disclosed and the right to verify and correct the data. The principle of fairness requires that the data collected is correct, is used for the purpose for which it is collected and is erased when the purpose is fulfilled.

5. Data Minimization – Data which is sought to be collected and processed ought to be minimal and necessary for the purpose(s) for which such data is sought. Sensitive personal data or information should only be allowed to be collected and processed for specific purposes and only if the purpose of collection and processing could not have been reasonably fulfilled by other means and should be deleted within a specified time period.

6. Data Controller Accountability – The Data Controller shall be responsible for maintaining the authenticity, integrity, confidentiality and security of the data collected by itself or entities with whom it may have shared the data for processing.

7. Regulatory Structure –Supervision and enforcement of the data protection law must be by an independent statutory authority with sufficient legal authority and technical capacity to enforce regulations. Given that data collection will be undertaken by public authorities under the executive, the statutory authority should function independent of executive control and maybe under parliamentary supervision. This may co-exist with appropriately decentralized enforcement mechanisms.

8. Deterrent penalties – penalties should be in the form of either corporal punishment or financial liability or both and should be imposed for the wrongful and unauthorized collection and processing of data. It must not only be adequate to ensure deterrence but also be benchmarked on the financial capacity of the violator and the magnitude of violation.

9. Best Practices Standard – the law must be technology agnostic. It must be flexible to taking into account changing technologies that aid in compliance. The law should only lay down the principles of regulation in terms of the rights and responsibilities of regulatees. The best technologies for aiding compliance would have to be developed as we go along. However the law should always promote a best practice of industry standard model of compliance technologies.

These principles shall be included as 'General Principles guiding data protection' in a separate chapter in the proposed Data Protection Law, so that same may be used to guide interpretative choices while interpreting the operative provisions of the statute.

III. SCOPE AND EXEMPTIONS

1. Territorial and Personal Scope

The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception since a single act of processing could very easily occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law.

Questions

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India?

Given that actions undertaken by private entities could impact the ability of Indians to exercise effective control over their personal information it is impossible to exclude such entities from being regulated under the Indian Data protection framework. This in itself provides a moral and ethical rationale for addressing the charge of extra territorial application.

Such entities which are not incorporated within the physical territory of India would still have to be regulated under Indian laws. The regulator will have to explore mechanisms of how to make them conform to Indian regulatory standards.

Existing legislation such as Section 3 and 4 of the Indian Penal Code provides for extraterritorial effect. So this is not something new or novel. Similar challenges are faced by other regulators such as in the pharmaceutical industry wherein regulatees are often situated beyond the national boundaries. This may be addressed through both internal and external measures such as greater international regulatory cooperation amongst national regulators.

2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

Law needs to be made applicable to such entities since the actions of such entities can directly cause harm to Indian residents. Harm is constituted by damage which results in physical or material injury or by any social or economic disadvantage.

3. While providing such protection, what kind of link or parameters or business activities should be considered?

Any business activity which involves the collection and processing of personal information of Indian residents should be regulated. This would include therefore all entities which may not have a presence in India but who by way of their activities can potentially cause harm to Indian residents. This would reflect similar rationale as that of the EU GDPR.

Alternatives:

a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.

b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR)

c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

4. What measures should be incorporated in the law to ensure effective compliance by foreign entities *inter alia* when adverse orders (civil or criminal) are issued against them?
A multiplicity of measures can be considered including blacklisting of violators, pursuing regulatory actions in partnership with other national regulators, actively advising Indian residents from entering into a contract with any entity which is in the list of violators, etc.

5. Are there any other views on the territorial scope and the extra-territorial application of a data protection law in India , other than the ones considered above?

2. Other Issues of Scope

There are three issues of scope other than territorial application. These relate to the applicability of the law to data relating to juristic persons such as companies, differential application of the law to the private and the public sector, and retrospective application of the law.

Questions

1. What are your views on the issues relating to applicability of a data protection law in India in relation to: (i) natural/juristic person; (ii) public and private sector; and (iii) retrospective application of such law?

The right to privacy is a facet of the fundamental right to life and personal liberty and can therefore only inhere in a natural person. The law should regulate personal information of natural persons alone. The rationale is also based on the fact that natural persons alone can suffer grave personal harm from loss of privacy and violation of personal information. Further statutory protection of data of juristic persons is already provided for under the IT Act and moreover the capacity of juristic persons to safeguard their personal data through contractual means is relatively much stronger than of natural persons, it is therefore the latter whose interests need to be given primacy in extending statutory protection through the data protection framework.

2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

Protecting data relating to juristic persons is already provided for under existing statutory legal instruments such as the IT Act and can be secured by way of private contracts and precious regulatory resources should not be spent on pursuing this goal.

3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

The law should be equally applicable to government and private entities collecting and processing personal information. For the government the collection and processing activities may be regulated via some specific provisions.

4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

The law should apply to processes such as storing, sharing, etc. irrespective of when data was collected.

5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

A transitional period should be provided (1 year) for all regulated entities to comply with provisions of the data protection law. SMEs may be provided longer transitional period and more regulatory advise vis-à-vis compliance strategies to be adopted.

3. Definition of Personal Data

The definition of personal information or personal data is the critical element which determines the zone of informational privacy guaranteed by a data protection legislation. Thus, it is important to accurately define personal information or personal data which will trigger the application of the data protection law.

Questions

1. What are your views on the contours of the definition of personal data or information?

Personal information should be information which is identifiable with a natural person, whether dead or alive. This would is a necessarily an all encompassing definition so as to include all aspects of information relating to an individual. It is difficult to provide an exhaustive definition of all kinds of personal information. The definition will necessarily have to be clarified through a case-by-case approach of applying this definition to specific instances. The aim is to provide as wide a coverage as possible to information relating to a natural person. The current definition of 'personal information' under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011, is adequate working definition.

2. For the purpose of a data protection law, should the term _personal data' or _personal information' be used?

The term personal information should be used as the word 'data' tends to obfuscate the nature of the information. Personal information also clearly alludes to the information generated about an individual, either by the individual or by another entity (whether government or private) but which nevertheless belongs to the natural person concerned.

Alternatives:
a. The SPDI Rules use the term sensitive personal information or data.

b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

Personal information would include biological facts, educational qualifications, photographs, other social identifiers like information on caste, ethnicity, race, economic status, sexual preference, gender and political interest or social interest affiliations. It will also include information generated (both directly and indirectly) by the person including blog posts, opinions, assessments (written, videography or photographs) which are shared on social media. It will also include tracking information in terms of information relating to the movement of the individual in both the physical space as well as the digital space.

4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an 'identified', 'identifiable' or 'reasonably identifiable', individual?

Personal information should be limited to information which is related to both an'identified' and 'reasonably identifiable' individual.

5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or psuedonymisation, for instance as the EU GDPR does?

Anonymisation is not a well established technology and there have been instances in the past where it has failed to secure the identity of the individual. It is therefore of limited efficacy and should be abandoned as a regulatory strategy. Pseudonymisation may one of the regulatory requirements which can be imposed on regulates.

[Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data. The EU GDPR actively recommends psuedonymisation of data.]

6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonablyidentifiable? What would be the standards of determing whether a person may or may not be identified on the basis of certain data?

No the standards of protection should not differ. There should be a regulatory presumption that all personal information is related to a reasonably indentifiable natural person and this should trigger the regulatory duties. It is for the regulatee to prove that the information does not relate to a reasonable identifiable natural person.

7. Are there any other views on the scope of the terms _personal data' and _personal information', which have not been considered?

4. Definition of Sensitive Personal Data

While personal data refers to all information related to a person‘s identity, there may be certain intimate matters in which there is a higher expectation of privacy. Such a category widely called _sensitive personal data‘ requires precise definition.

Questions
1. What are your views on sensitive personal data?

There should be absolute prohibition on the collection and processing of sensitive personal information unless express informed consent is taken for a limited purpose in providing specific services to the individual. The category of sensitive personal information includes financial, sexual orientation, health, caste, ethnic and race, educational qualifications, political and religious belief and affiliations. The individual should also be able to exercise greater control in denoting specific information as “”sensitive personal information”, this will also allow the “reasonable expectation of privacy” standard to be addressed subjectively from the point of view of the individual concerned.

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg.Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?

Yes the law should define a set of information as ‘sensitive personal information’ and lay down a default rule of prohibition on the collection and processing of such information unless specifically and expressly consented by the individual concerned. Moreover the definition of ‘sensitive personal information’ can on specific instances be extended to include other information which the individual would like to be denoted as such so as to attract protection of the prohibitory standard.

[For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]
3. Are there any other views on sensitive personal data which have not been considered above?
None

5. Definition of Processing
Data protection laws across jurisdictions have defined the term _processing‘ in various ways. It is important to formulate an inclusive definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law.
For a fuller discussion, see page 44 above.

Questions
1. What are your views on the nature and scope of data processing activities?

Data collection and data processing should be distinguished. An inclusive and wide definition should be provided for data processing activities. Data collection refers to the collection of personal information with the intention of storage and further processing of such personal information for commercial or professional purposes. Data processing includes working on personal information in a manner which allows such information to be sifted, re-categorized, repurposed (including entailing disclosure) for commercial or professional purposes. It is possible to imagine that the same entity both collects and processes personal information. However this may not necessarily be true in all cases. Regulatory duties and responsibilities need to be specified for both data collectors and data processors.

2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?
Data collection should be defined as the collection of data with the aim of processing of that data for the commercial or profeessional purposes. Data processing is the working of the personal information collected. It is important to note that there is no possibility of benign collection of personal information. Personal information is always collected with the aim of processing that information to generate further goods and services and in the realization of greater commercial benefits to the data collector.

3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

The law should apply to both automated and manual processing because otherwise this will create a loophole that will enable regulatees to escape by falsely claiming that data collected is only being manually processed and to later change their mind to allow for automated processing of data. It is impossible for the regulator to *suo moto* track when such a decision is made thereby exponentially increasing the risk of unauthorized disclosure of the data. The regulatory burden should not differ between those choosing manual and automated processing of data. All personal information should therefore be included, howsoever it may be processed.

Alternatives:
a. All personal data processed must be included, howsoever it may be processed.
b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.
c. Limit the scope to automated or digital records only.

4. Are there any other issues relating to the processing of personal data which have not been considered?
None

6. Definition of Data Controller and Processor

The obligations on entities in the data ecosystem must be clearly delineated. To this end a clear conceptual understanding of the accountability of different entities which control and process personal data must be evolved.
For a fuller discussion, see page 48 above.

Questions
1. What are your views on the obligations to be placed on various entities within the data ecosystem?

There should be different legal obligations placed on the data collector and the data processor. As discussed above in some cases, the data collector and data processor may be the same entity but this may not necessarily be true in all cases. Therefore legal responsibilities need to be differentiated between the data collector and the data processor. The law needs to define the legal responsibilities of data collector and data processor separately.

2. Should the law only define 'data controller' or should it additionally define 'data processor'?

Alternatives:
a. Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable.
b. Use the concept of _data controller‘ (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
c. Use the two concepts of _data controller‘ and _data processor‘ (entity that receives information) to distribute primary and secondary responsibility for privacy.

3. How should responsibility among different entities involved in the processing of data be distributed?

Alternatives:
a. Making data controllers key owner and making them accountable.

b. Clear bifurcation of roles and associated expectations from various entities.
c. Defining liability conditions for primary and secondary owners of personal data.
d. Dictating terms/clauses for data protection in the contracts signed between them.
e. Use of contractual law for providing protection to data subject from data processor.

4. Are there any other views on data controllers or processors which have not been considered above?

7. Exemptions

Exemptions from legal obligations can be provided for collection of data for personal and household uses, exemption for academic research, journalism. Non-consensual collection of data may be allowed in public emergencies and in specific instances in the public interest (such instances should be specified in the legislation itself) by public authorities. However even in such cases, there should not be excessive delegation of such responsibilities to third parties which are non-governmental,so as to ensure that data is safeguarded and such powers are held and exercised by a high ranking public official.

8. Cross Border Flow of Data

9. Data Localisation

10. Allied Laws

The Data Protection Law would be an overarching comprehensive statute governing all instances of collection and processing of data and it should contain a clause stating that the general principles governing data protection are applicable to all other extant legislations governing the collection and processing of data.

IV. Grounds of Processing, Obligations on Entities and Individual Rights

The General Principles provided in Section II of this paper, refers to specific aspects of data authorship, individual consent, responsibility of data collector and transparency which will together ensure that individual rights in the context of all aspects of data collection and processing are protected and safeguarded.

V. Regulation and Enforcement

Principle 7 of the General Principles provided in Section II states that the supervision and enforcement of the data protection law must be by an independent statutory authority with sufficient legal authority and technical capacity to enforce regulations. Given that data collection will be undertaken by public authorities under the executive, the statutory authority should function independent of executive control and maybe under parliamentary supervision. This may co-exist with appropriately decentralized enforcement mechanisms.